Sanford P. Dumain (*pro hac vice*)
Peter E. Seidman (*pro hac vice*)
Melissa Ryan Clark (*pro hac vice*)
Charles Slidders (*pro hac vice*)
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, NY 10119
Telephone: (212) 594-5300
Fax: (212) 868-1229
sdumain@milberg.com
pseidman@milberg.com
mclark@milberg.com
cslidders@milberg.com

Joseph H. Malley (*pro hac vice*)
LAW OFFICE OF JOSEPH H. MALLEY, P.C.
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100
Fax: (214) 943-6170
malleylaw@gmail.com

David C. Parisi (SBN 162248)
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, CA 91403
Telephone: (818) 990-1299
Fax: (818) 501-7852
dparisi@parisihavens.com

Counsel for Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

MATTHEW HINES, JENNIFER AGUIRE, and ALEXANDER HERNANDEZ, individually and on behalf of all others similarly situated, Plaintiffs, v. OPENFEINT, INC., a Delaware Corporation, and GREE INTERNATIONAL, INC., a California Corporation. Defendants.	Case No. 11-cv-3084-EMC JURY TRIAL DEMANDED **AMENDED CLASS ACTION COMPLAINT FOR:** 1) An Accounting; 2) Violations of 18 U.S.C. § 2701, *et seq.*, the Stored Commc'ns Act; 3) Violations of Cal. Civ. Code § 1798.80, Consumer Legal Remedies Act; and 4) Negligence.

Plaintiffs Matthew Hines and Alexander Hernandez, on behalf of themselves and all others similarly situated, by and through their attorneys, Milberg LLP, the Law Office of Joseph H. Malley, P.C., and Parisi & Havens LLP, allege the following based upon information and belief, based on, *inter alia*, investigation conducted by and through their attorneys; Plaintiffs' allegations as to themselves and their own actions are based upon their personal knowledge.

NATURE OF THE ACTION

1. Plaintiffs bring this action on behalf of themselves and a class of similarly situated mobile device owners who used OpenFeint-affiliated applications (or "apps") and who were victims of privacy violations (the "Class"). Class members' privacy and security rights were violated by Defendant OpenFeint, Inc. because Defendant:

- Collected and stored Class members' personally identifiable information, including customized account names, GPS "Fine" coordinates (i.e., the exact latitude and longitude of users' location), and Facebook and Twitter profile information;
- Associated that information with the unique device identifiers ("UDIDs") from Class members' mobile devices, which are used by myriad companies to track behavioral and usage data for advertising and marketing purposes; and
- Without Plaintiffs' knowledge or consent, made that personally identifiable information available to third parties, allowing the UDIDs to be de-anonymized (i.e., associated with their personal identities), thereby connecting Plaintiffs' and Class members' identities with thousands of databases of information containing their mobile device usage and behaviors as well as other private information.

2. Defendant made Plaintiffs' and Class members' personally identifiable information was made publicly available, in unencrypted form.[1] OpenFeint did not require that the request for information be made via a mobile device, and instead allowed anyone to access Plaintiffs' personally identifiable information regarding a UDID by accessing OpenFeint's servers through a web browser without the need for a username or password. Although tests show that OpenFeint may have stopped divulging certain information as of April 2011—like

[1] In the context of this Complaint, the term "unencrypted" means that the data divulged was not coded, i.e., it was written in plain English. Plaintiffs make no allegations regarding encryption of data while it was "on the wire," i.e., *during* the seconds or milliseconds that it was in transmission.

GPS coordinates and social media profiles—Defendant OpenFeint continues to publicly divulge personally identifiable information like the users' customized account names.

INTRADISTRICT ASSIGNMENT

3. Defendant OpenFeint, Inc. is a wholly-owned subsidiary of GREE International, Inc. Its principal executive offices and headquarters are located in this District at 330 Primrose Road, Burlingame, California. Intra-district assignment to the San Francisco Division is proper.

JURISDICTION AND VENUE

4. This Court has diversity jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and 1332(d), because the amount in controversy exceeds $5,000,000.00, exclusive of interests and costs, and there is at least minimal diversity between the members of the Class and Defendant. This Court also has federal question jurisdiction under 28 U.S.C. § 1331, as this action arises in part under a federal statute, the Electronic Communications Privacy Act, and in particular, the Stored Communications Act. This Court also has personal jurisdiction over Defendant because it maintained its corporate headquarters in this state, a substantial portion of the wrongdoing alleged took place in this state, Defendant conducts business in this state, and Defendant has sufficient minimum contacts with this state and/or otherwise intentionally availed itself of the markets in this state through the promotion, marketing, sale, and use of its products and services in this state.

5. Venue for this action properly lies in this District pursuant to 28 U.S.C. § 1391, as Defendant's principal executive offices and headquarters are located in this District, Defendant conducts business and has significant contacts with this District, and a substantial portion of the events and conduct giving rise to the violations of law complained of herein occurred in this District.

PARTIES

Plaintiffs

6. Plaintiff **Matthew Hines** is a citizen and resident of Fort Worth, Texas, (Tarrant County, Texas). Mr. Hines used an Apple iPhone to download, install, and access OpenFeint-affiliated applications, including, for example Deer Hunter: African Safari, Doodle Army, and

Fall Guy. Mr. Hines' OpenFeint account contained personal, private information, including his customized OpenFeint account name, Facebook account, information, and information about the games he played.

7. Plaintiff **Alexander Hernandez** is a citizen and resident of Dallas, Texas, (Dallas County, Texas). Mr. Hernandez used an Apple iPhone to download, install, and access OpenFeint-affiliated applications, including, for example, Amazing X-Ray FX Lite, Glass Tower, Minesweeper, and Applets. Mr. Hernandez's OpenFeint account contained personal, private information, including his customized OpenFeint account name, GPS location, and information about the games he played.

8. Plaintiffs each used their mobile devices to access, on one or more occasions, one or more applications that are affiliated with Defendant OpenFeint (i.e., that use OpenFeint's software platform to provide social media functions to the application, and which communicate with OpenFeint's servers upon start-up). Defendant OpenFeint collected and stored personally identifiable information regarding Plaintiffs and allowed that information to be accessed by anyone—in connection with their UDID. This information leak allowed Plaintiffs' and Class members' UDIDs—which are stored on countless databases with what would otherwise be anonymous data—to be de-anonymized and associated with their actual identities.

9. Plaintiffs and Class members value the privacy of their UDID, as well as the information associated with their OpenFeint accounts, including their personally identifiable information. They consider this information of a private, confidential, and sensitive nature, and did not want this information divulged to third parties.

10. The information OpenFeint disclosed is an asset of Plaintiffs' and Class members as to which third parties have no right to access. Plaintiffs and Class members reasonably expected that any data accessed by OpenFeint would be protected, encrypted, and not divulged to third parties.

Defendant

11. Defendant **OpenFeint, Inc.** is a Delaware corporation which maintains its headquarters at 330 Primrose Road, Burlingame, Suite 515, California, (San Mateo County, California). Defendant OpenFeint conducts business throughout the United States, in the State of California, and in this judicial district.

12. Defendant OpenFeint claims to be "the largest mobile social gaming network for iOS [Apple's mobile operating system] & Android devices on the planet." OpenFeint allows application developers to add social network aspects to their games, and also provides a network to advertise other OpenFeint-enabled games

FACTUAL ALLEGATIONS

Defendant OpenFeint

13. Defendant OpenFeint provides tools that enable application developers to easily add social media aspects to their mobile device games and other applications.[2] These social media aspects include the ability to chat, identify nearby friends and application users, and import information from and share information with Facebook and Twitter accounts. OpenFeint is the largest mobile social gaming network, and is affiliated with more than 5,300 gaming applications involving 100,000,000 users.

14. Many of Defendant OpenFeint's games target children, and are rated 4+ for ages four and up, 9+ for ages nine and up, and 12+ for ages twelve and up. These apps are marketed to minor children with storybook tales, friendly animals, and child-like game scenarios.

15. The UDID was originally designed to allow application developers to identify each unique phone, so that the applications could store and associate application preferences or history. Defendant OpenFeint uses mobile devices' UDIDs to collect and track information

[2] An application, or "app," is software which helps a user perform specific tasks, as opposed to software that manages a computer's (or mobile device's) basic capabilities. Apps include games, media players, mapping programs, accounting programs, and the like.

regarding user preferences, high scores, and locations from the various OpenFeint-affiliated applications associated with any one UDID.[3]

16. When Plaintiffs and Class members—or their children—used any one of the thousands of OpenFeint-affiliated application, their mobile device communicated with OpenFeint's servers as follows:

- When Plaintiffs downloaded and opened their first OpenFeint-affiliated application, the device (e.g., mobile phone) communicated with OpenFeint's servers. Through that communication, OpenFeint logged (stored) the mobile device's UDID, returned a temporary username, and stored the UDID and temporary username together—creating Plaintiffs' OpenFeint account.

- Then, Plaintiffs were prompted to customize their usernames, and engage other social media features by, for example, linking their OpenFeint profile to their Facebook account, or by adding friends.

- After this initial set-up, any time Plaintiffs used an OpenFeint-affiliated application, their mobile device (prompted by the application) sent a "call" to OpenFeint's servers, seeking any accounts associated with the UDID.

- The OpenFeint server responds to the "call" by returning accounts associated with the UDID. Because UDIDs are permanent, this "call" could return usernames from previous owners or other users of the phone. Plaintiffs can then select which username (as provided by OpenFeint or customized by the user) belongs to him or her, thereby logging in.

- OpenFeint also responded to the call with a wealth of unencrypted, stored information associated with the UDID, including, for example, customized username, latitude and longitude, and a URL to a Facebook profile picture.

- No password, entry of the username, key, or other verification is required in this process; the call is thus entirely "unauthenticated." Defendant OpenFeint also fails to encrypt the information sent to or from its servers or verify that the call is coming from a mobile device and through an OpenFeint-affiliated application.

[3] Every Apple iPhone, iPad, and iPod Touch, shipped since the iPhone's introduction in 2007, contains a UDID, which is a unique serial number, visible only to software. UDIDs are hard coded into a user's phone software, meaning that they cannot be changed or deleted, and are forever associated with the mobile device.

OpenFeint Allows Third Parties to De-Anonymize UDIDs

17. During this process, OpenFeint laid users' information bare, divulging a wealth of personally identifiable, private information. On May 4, 2011, Aldo Cortesi, a coder and security consultant in New Zealand, published an article entitled "De-anonymizing Apple UDIDs with OpenFeint." In that article, Cortesi demonstrated how he could send a request for information to OpenFeint's servers by supplying his UDID from a web browser, and receive substantial personal information including: his latitude and longitude, the last game he played, his account name, and his Facebook profile picture URL. Not only did the Facebook profile picture URL divulged by OpenFeint lead to a picture of Cortesi, the URL itself contained Cortesi's Facebook user ID, which leads to his Facebook profile.

18. As outlined in the Cortesi article, this personal information could be accessed by typing a UDID into https://api.openfeint.com/users/for_device.xml?udid=XXX (replacing "XXX" with the UDID).

19. Cortesi did not have to enter a password, username, or any other authentication key, and did not even have to send the request from a mobile device, let alone *his* mobile device. OpenFeint also failed to require any age verification, and thus exposed the personally identifiable information and exact location of users' who downloaded OpenFeint-affiliated applications, including those targeted at children as young as four years old.

20. A May 9, 2011, CNN Tech article entitled "Researchers: iPad, iPhone IDs can give away identities," addressed the importance of keeping UDIDs anonymous, stating, in part:

> By itself, the UDID doesn't expose personal data, but to the extent that it's tied to other information about the phone's user, it can function like a permanent, ineradicable "evercookie." In theory, that could allow advertisers or other parties to track a wide variety of your activities through your smartphone . . . .
>
> This identifier is at the center of criticism amid growing concerns about smartphone privacy. The Wall Street Journal last year conducted independent tests and found that out of 101 apps, 56 transmitted the device's UDID to other companies without user awareness or consent. . . .
>
> "[UDIDs are] permanent Social Security numbers in your phone that are freely transmitted and can't change," said Justin Brookman, director of the Center for Democracy and Technology's consumer privacy project.

21. Defendant OpenFeint's misconduct has a reach that extends leaps and bounds: Because Defendant OpenFeint reveals this personally identifiable information in connection with the mobile device's UDID, the UDID is no longer just a number; anyone, be it a stranger or large marketing and data aggregation corporation, can put a name to it and the private information correlated with a previously-anonymous UDID. And because many OpenFeint games are targeted at children, the personally identifiable information—including the GPS location—of minor children is also revealed.

22. In response to Cortesi's article, Defendant OpenFeint purportedly stopped transmitting some of the personally sensitive and identifiable data—specifically, GPS coordinates and Facebook profile/picture information. However, OpenFeint still associates and stores Plaintiffs' and Class members' UDIDs with this information, as well as other private user information including the last game played, whether they are logged in to the OpenFeint network, profile pictures, and user-chosen account names (which can often be used to identify users). It also still *publicly* associates Plaintiffs' and Class members' UDIDs with information about their OpenFeint account and application use, including, for example, their customized account name — which frequently references one's actual name and/or is used across a variety of websites and services, including email accounts, banks, and message forums.

23. Defendant OpenFeint is no stranger to user tracking without notice or consent; its predecessor, Aurora Feint, was suspended from a mobile app store in 2008 over privacy concerns.[4] When Aurora Feint users opted into that service's "community" feature, Aurora Feint obtained the user's contact list, sent it unencrypted to its servers, and matched the user with their friends who were currently playing games. In response to privacy concerns, Aurora Feint stated:

> **When we discovered that the Apple SDK [software development kit] allowed us to look through your contact list we thought it would be a great idea to automatically show you which friends are playing the game.** Why automatically? Well,

[4] Jason Chen "Aurora Feint iPhone App Delisted for Lousy Security Practices" June 23, 2008, (last accessed May 28, 2011) online: http://gizmodo.com/5028459/aurora-feint-iphone-app-delisted-for-lousy-security-practices

> everyone always complains about the keyboard on the iPhone and how annoying it is to type on it. So we thought, "Hey, why don't we make this feature REALLY easy to use – no typing!" And such, the community feature was born. **Some people have said that it would have been ok if we had a better notice explaining what was going on.** I agree! We weren't trying to be sneaky about how this worked. It was just overlooked. No one we showed it to even asked a question about it – nor did we. It just simply never came up as a potential issue when we beta tested the game with early users.

(Emphasis added.)

24. Most Defendant OpenFeint-affiliated applications provide no terms of service, no privacy policy, and no link to a website with such information. Defendant OpenFeint also fails to provide a link to its terms of service or privacy policy within its platform. Plaintiffs and Class members were never informed that their OpenFeint account information or other personally identifiable information was being disclosed, let alone with their UDID, and never consented to or had an opportunity to opt-out of this misconduct.

The Value of Personal Information

25. Hundreds, if not thousands, of different companies, including game application developers, web analytics companies, and advertisers, aggregate user information and correlate that information with anonymous UDIDs. Web analytics companies have software platforms that are embedded in hundreds of thousands of applications; store terabytes (or more) of information; analyze billions of different data points and unique events within application sessions; aggregate the data-set they obtain from across this variety of applications; and create demographic profiles regarding user interests for market segmentation and marketing campaigns. *See, e.g.,* http://www.flurry.com/data/index.html. Once OpenFeint allowed the de-anonymization of Plaintiffs' and Class members' UDIDs, these analytics companies had the ability to place an actual identity, as well as other, key demographic information, with the information the analytics companies had aggregated regarding users' demographics and behavior.

26. The information OpenFeint wrongfully divulged was a commodity that could be valued by reference to unit price. For example, on March 7, 2011, the *Wall Street Journal*

published an article under the headline, "Web's Hot New Commodity: Privacy" in which it highlighted a company called "Allow Ltd.," one of nearly a dozen companies that offer to sell people's personal information on their behalf, and giving them 70% of the sale. One Allow Ltd. customer received payment of $8.95 for letting Allow tell a credit card company he is shopping for new credit. In January 2011, at the World Economic Forum in Davos, Switzerland, one discussion centered on turning personal data into an "asset class." During the course of the discussion, Michele Luzi, director at consulting firm Bain & Co. stated, "We are trying to shift the focus from purely privacy to what we call property rights." *Id.*; *See also,* Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 29, 2009), *available at* http://ssrn.com/abstract=1478214 (**"Websites and stores can, therefore, easily buy and sell information on visitors with the intention of merging behavioral with demographic and geographic data in ways that will create social categories that advertisers covet and target with ads tailored to them or people like them."**) (emphasis added); Federal Trade Commission Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change* (Dec. 2010), at 24 ("FTC Report") (**"the more information that is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him."**) (emphasis added); *See also* MediaPost, http://www.mediapost.com/events/?/showID/OMMAGlobalNewYork.09.NewYorkCity/type/Exhibitor/itemID/647/OMMAGlobalNewYork-Exhibitors%20and%20Sponsors.html (last visited Aug. 3, 2011).

Plaintiffs and Class members Suffered Financial Harm

27. Defendant impaired Plaintiffs' and Class members' ability to sell their mobile devices. Because OpenFeint connects personal, private information with the mobile devices' permanent UDIDs, and releases that information in connection with unauthenticated calls, mobile device owners risk having future owners access their private information. For example, if Owner 1 is an OpenFeint user, and sells his phone to Owner 2, when Owner 2 opens any OpenFeint-affiliated application, s/he will be allowed to select and access Owner 1's OpenFeint account—which includes personal data regarding, for example, Facebook and Twitter accounts,

friends, and message board postings. In addition, if they sell or transfer their mobile devices, Plaintiffs and Class members' risk having their personal identities associated with another, future users' application use, behavioral data, and other aggregated data that will continue to be correlated with the UDID which OpenFeint allowed to be associated with each Plaintiff's and Class member's actual identity.

28. Defendant also deprived Plaintiffs and the Class members of the right to decide if and when they divulge their personal information in connection with their UDID, and usurped the property interest that Plaintiffs and Class members' hold in their UDIDs, personal identities, account information, and mobile device and application use behavior, which is marketable, valuable information.

CLASS ALLEGATIONS

29. Pursuant to Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiffs bring this action as a Class action, on behalf of themselves and all persons who downloaded and enabled a mobile applications affiliated with OpenFeint, i.e., using the OpenFeint platform/software, since OpenFeint's launch on or around February 17, 2009, to the date of the filing of this complaint (the "Class).

30. Plaintiffs reserve the right to revise the definitions of the Class based on facts learned in the course of litigation of this matter and through discovery.

31. Plaintiffs seek equitable relief, damages, and injunctive relief including an accounting of the recipients of their personal information, pursuant to:

a) Stored Communications Act, 18 U.S.C. § 2701, *et seq.*;

b) California Civil Code § 1798.80 - Security Requirements for Customer Records; and

c) Common Law Principles of Negligence.

32. **Persons Excluded From Class:** Specifically excluded from the proposed Class are Defendant, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint ventures, or entities controlled by Defendant, and their heirs, successors, assigns, or other persons or entities related to or affiliated

with Defendant and/or their officers and/or directors, or any of them; the Judge assigned to this action, and any member of the Judge's immediate family.

33. **Numerosity:** The members of the Class are so numerous that their individual joinder is impracticable. Plaintiffs are informed and believe, and on that basis allege, that the proposed Class contains tens of thousands of members. The precise number of Class members is unknown to Plaintiffs. The true number of Class members is known by Defendant, however and, thus, Class members may be notified of the pendency of this action by first Class mail, electronic mail, and by published notice. Upon information and belief, Class members can be identified by the electronic records of Defendant.

34. **Class Commonality:** Pursuant to Federal Rules of Civil Procedure, Rule 23(a)(2) and Rule 23(b)(3), are satisfied because there are questions of law and fact common to Plaintiffs and the Class, which common questions predominate over any individual questions affecting only individual members. The common questions of law and factual questions include, but are not limited to:

a) Whether OpenFeint divulged and/or shared personal and/or account information about Plaintiffs and the Class to/with third parties;

b) Whether OpenFeint allowed UDIDs to be de-anonymized;

c) What information about a user and/or his/her OpenFeint account OpenFeint disclosed to third parties;

d) Whether users ever received notice of Defendant's business practice of revealing their private account information and/or personally identifiable information to third parties;

e) Whether users ever had the opportunity to and/or did consent to Defendant's business practice of revealing their private account information and/or personally identifiable information to third parties;

f) Whether Defendant's privacy policies created any understanding that OpenFeint-affiliated application users' personal and/or private account information would be protected from disclosure to third parties;

g) Whether Defendant's business practices, as alleged herein, violated the Stored Communications Act;

h) Whether Defendant's business practices, as alleged herein, violated California Civil Code § 1798.80 - Security Requirements for Customer Records;

i) Whether Defendant was negligent in allowing user information to be disclosed and/or divulged to third parties;

j) Whether Plaintiffs and members of the Class have sustained damages as a result of Defendant's conduct, and, if so, the appropriate measure of damages;

k) Whether Plaintiffs and members of the Class are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

l) Whether Plaintiffs and members of the Class are entitled to punitive damages, and, if so, the amount.

35. **Typicality:** Plaintiffs' claims are typical of the claims of all of the other members of the Class, because his claims are based on the same legal and remedial theories as the claims of the Class and arise from the same course of conduct by Defendant.

36. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the interests of the members of the Class. Plaintiffs have retained counsel highly experienced in complex consumer Class action litigation, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

37. **Superiority:** A Class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members is relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against the Defendant. It would thus be virtually impossible for the Class, on an individual basis, to obtain effective redress for the wrongs done to them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the Class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive

supervision by a single court, and presents no unusual management difficulties under the circumstances here.

38. In the alternative, the Class may be also certified because:

a) the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudication with respect to individual Class members that would establish incompatible standards of conduct for the Defendant;

b) the prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

c) Defendant have acted or refused to act on grounds generally applicable to the Class thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

39. The claims asserted herein are applicable to all persons throughout the United States that meet the class definition and class period.

40. The claims asserted herein are based on Federal law and California law, which is applicable to all Class members throughout the United States.

41. Adequate notice can be given to Class members directly using information maintained in Defendant's records or through notice by publication.

42. Damages may be calculated from the information maintained in Defendant' records, so that the cost of administering a recovery for the Class can be minimized.

FIRST CAUSE OF ACTION

For an Accounting of the Unauthorized Recipients of Plaintiffs' Data

43. Plaintiffs and the Class members seek an accounting of all persons, entities, servers, devices, IP addresses, or the like, other than Defendant OpenFeint, to whom or to which OpenFeint revealed Plaintiffs' and Class members' valuable personal and private data as alleged herein.

44. Plaintiffs and the Class members entrusted Defendant with their personal, private information and data.

45. Plaintiffs and the Class members have a direct interest in their data and information, as it relates both to their privacy and to their personal, commercial property.

46. The recipients of Plaintiffs' and Class members' personal and private data are unknown to them and cannot be ascertained without a judicial accounting.

SECOND CAUSE OF ACTION
Violations of 18 U.S.C. § 2701, *et seq.*
The Stored Communications Act

47. Plaintiffs incorporate by reference all paragraphs previously alleged herein.

48. Defendant provides an electronic communication service to the public because it provides to its users the ability to send or receive wire communications (i.e., aural transfers made through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection) and electronic communications. (i.e., the transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire system that affects interstate or foreign commerce). Defendant received and stored electronic communications from Plaintiffs and Class members; the only intended recipients of these electronic communications were application developers that used OpenFeint's platform, and whose applications were downloaded to and installed on the mobile devices of Plaintiffs and Class members. Defendant OpenFeint was not an intended recipient of these electronic communications, and received and stored the communications only in its capacity as an electronic communication and remote computing service.

49. Defendant also provides a remote computing service to the public because it provides computer storage or processing services by means of an electronic communications system.

50. Defendant carries and maintains users' UDID and private information solely for the purpose of providing storage and computer processing services. Defendant is not authorized to divulge this information or to access this information for purposes other than providing storage and computer processing.

51. Class members' UDIDs, OpenFeint account information, and other personally identifiable information as discussed herein, are electronic communications within the meaning of 18 U.S.C. § 2510 (12).

52. Defendant holds these UDIDs, OpenFeint account information, and other personally identifiable information as discussed herein in electronic storage within the meaning of 18 U.S.C. § 2510(17).

53. Defendant knowingly, willfully, unlawfully, and intentionally without authorization divulged confidential and private information relating to Plaintiffs' electronic communications.

54. Defendant engaged in the foregoing acts without obtaining the lawful consent of the user.

55. Each Plaintiff and Class member is entitled to statutory damages of no less than $1,000. Plaintiffs and the Class are also entitled to equitable or declaratory relief; reasonable attorney's fees and other litigation costs; and punitive damages.

THIRD CAUSE OF ACTION
Violation of California Civil Code §1798.80
Security Requirements for Customer Records

56. Plaintiffs fully incorporate by reference herein all of the above paragraphs, as though fully set forth herein.

57. Cal. Civ. Code § 1798.82 requires any business that owns or licenses computerized data that includes personal information to "disclose any breach of the security of the system following discovery or notification of the breach . . . whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person . . . in the most expedient time possible and without unreasonable delay."

58. Defendant failed to disclose to Plaintiffs and the Class, in the most expedient time possible and without unreasonable delay, the breach of security that exposed users' OpenFeint account information and personally identifiable data and which allowed their UDIDs to be de-anonymized.

59. Defendant learned of the breach on or before April 5, 2011, but failed to publicly disclose that consumer data was acquired by and disclosed to unauthorized third parties.

60. Defendant also failed to publicly disclose that users' personally identifiable information was not encrypted, and thus more vulnerable to exploitation.

61. Defendant has not taken reasonable steps to ensure that all OpenFeint-application users are informed of the security breach. As a result, many Class members may still be unaware that their data has been compromised.

62. As a direct and proximate result of Defendant' acts and omissions described herein, Plaintiffs and the Class have suffered damages including, but not limited to, invasion privacy, loss of property, loss of money, loss of control of their personal financial and other nonpublic information, identity theft, and the burden of monitoring their financial and credit accounts, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
Negligence

63. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

64. As set forth above, OpenFeint owed a duty to Plaintiffs and Class members.

65. OpenFeint breached its duty by designing a mobile platform so that the application developers, advertising affiliates, and other third parties could acquire personal information without consumers' knowledge or permission and by constructing and controlling consumers' user experience and mobile environment so that consumers could not reasonably avoid such privacy-affecting actions.

66. OpenFeint failed to fulfill its own commitments and, further, failed to fulfill even the minimum duty of care to protect Plaintiffs' and Class members' personal information, privacy rights, and security.

67. OpenFeint's failure to fulfill its commitments included its practice of capturing frequent and detailed information about users' GPS "Fine" locations for unreasonable retention periods, maintaining records of such location histories on users, divulging such location history

files to users' mobile device, divulging such location history files to other mobile devices with which users synchronized their mobile devices, storing such location history files in accessible, unencrypted form, and allowing third parties to access such information.

68. OpenFeint negligently stored, received, and sent data and electronic communications in unencrypted form, and sent unencrypted stored data, including personally identifiable information, to third parties, without any verification or authentication that the third parties were the user, an OpenFeint-affiliated application developer, or any authorized third party. Defendant OpenFeint failed to encrypt data, require a password, verify that requests were coming from a mobile device (let alone the mobile device actually associated with the UDID), or verify the age of users whose personally identifiable information OpenFeint stored and later divulged.

69. Plaintiffs and Class members were harmed as a result of OpenFeint's breach of its duties, and OpenFeint proximately caused such harms.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, prays for judgment against Defendant as follows:

A. Certify this case as a Class action on behalf of the Class defined above, appoint Plaintiffs as Class representatives, and appoint their counsel as Class counsel;

B. Declare that the actions of Defendant, as set out above, violate the alleged causes of action.

C. And award Plaintiffs and Class members:

1) Damages, including statutory damages where applicable, to Plaintiffs and Class members in an amount to be determined at trial;

2) Restitution against Defendant for all money to which Plaintiffs and the Class are entitled in equity;

3) Declaratory and injunctive relief including, but not limited to, an order required Defendant to:

a) Cease disclosing OpenFeint users' personal and/or private information to any and all third parties, other than disclosure to authenticated, verified account holders or application developers,

in an encrypted form, when necessary to perform the services that OpenFeint provides;

b) Verify that calls for account information are initiated from the actual mobile device associated with the UDID for which information is requested and from a OpenFeint-affiliated application before responding;

c) Require password authentication before sending any personal and/or private data;

d) Require age verification before sending any personal and/or private data; and

e) Encrypt all incoming and outgoing data to OpenFeint servers.

4) An accounting of all persons, entities, IP addresses, devices, or the like, that were allowed unauthorized access to Plaintiffs' and Class members' personal and/or private data by OpenFeint and/or to whom OpenFeint sold or marketed personal and/or private data ascertained through OpenFeint-affiliated applications;

5) Reasonable attorneys' fees and costs;

6) Such other and further relief as this Court may deem just and proper.

Dated: September 6, 2011

/s/ Peter E. Seidman

Sanford P. Dumain (*pro hac vice*)
Peter E. Seidman (*pro hac vice*)
Melissa Ryan Clark (*pro hac vice*)
Charles Slidders (*pro hac vice*)
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, NY 10119
Telephone: (212) 594-5300
Fax: (212) 868-1229
sdumain@milberg.com
pseidman@milberg.com
mclark@milberg.com
cslidders@milberg.com

Joseph H. Malley (*pro hac vice*)
LAW OFFICE OF JOSEPH H. MALLEY, P.C.
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100
Fax: (214) 943-6170
malleylaw@gmail.com

David C. Parisi (SBN 162248)
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, CA 91403
Telephone: (818) 990-1299
Fax: (818) 501-7852
dparisi@parisihavens.com

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and service will be accomplished via the CM/ECF system

Date: September 6, 2011

/s/
Peter Seidman